IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH frankhugginse5@yahoo.com THAT IS STORED AT PREMISES CONTROLLED BY OATH INC. D/B/A VERIZON MEDIA, 701 FIRST AVENUE, SUNNYVALE, CALIFORNIA 94089	Case No. 20-SW-2136DPR **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nick Masellis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Oath Inc. d/b/a Verizon Media, an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California, 94089, a location within the Northern District of California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath Inc. d/b/a Verizon Media to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Defense Criminal Investigative Service ("DCIS") and have been since January 7, 2018. From my work with DCIS I have become familiar with the methods in which the United States military and civilian agencies procure goods and services,

including the types of authorizations and records that are required for the military to purchase goods and services. Through this work, I have gained training and experience conducting investigations into crimes involving wire fraud, conspiracy, false claims, and money laundering, to include training and experience applying for and executing search warrants. I have assisted in the preparation of affidavits to support the establishment of probable cause for search warrants. During the course of this investigation and in my preparation of this application and affidavit, I have consulted with other DCIS agents and other law enforcement personnel who have applied for search warrants of e-mail accounts. I am familiar with the facts set forth below based upon my investigative findings and information provided by other participating law enforcement agents.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 287 (false claims), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1956 (money laundering), and 18 U.S.C. § 1957 (money laundering) have been committed by Franklin Huggins ("Huggins"), and that Huggins used the following e-mail address in committing these crimes: frankhugginse5@yahoo.com ("Subject Account"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction

over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

6. Title 18, United States Code, Section 287 provides that,

Whoever makes or presents to any person or officer in the civil, military, or naval service of the United States, or to any department or agency thereof, any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false, fictitious, or fraudulent, shall be imprisoned not more than five years and shall be subject to a fine in the amount provided in this title.

7. Title 18, United States Code, Section 371 provides that,

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

8. Title 18, United States Code, Section 1343 provides that,

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

9. Title 18, United States Code, Section 1956 provides, in pertinent part, that,

(a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity –

(A) (i) with the intent to promote the carrying on of specified unlawful activity; or
(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part –
(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both . . . .

10. Title 18, United States Code, Section 1957 provides, in pertinent part, that,

(a) Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished . . .

. . .

(d) . . . (1) that the offense under this section takes place in the United States . . . .

PROBABLE CAUSE

11. The United States Army Directorate of Family and Morale, Welfare and Recreation ("MWR") manages programs and services that support readiness and resilience for soldiers and families. These services include providing annual transportation for military service members during the Christmas holidays. The service, known as "Exodus," provides bus transportation to airports so that military service members can be with their families during the holidays.

12. Vandalia Bus Lines, Inc. ("Vandalia"), of Caseyville, Illinois, is a family-owned charter bus company that provides motor coach transportation. Vandalia is a contractor for the United States Department of Defense and provides transport for military personnel. Vandalia had a Memorandum of Agreement ("MOA"), in lieu of contract, with the Fort ("Ft.") Leonard Wood MWR for holiday "Exodus" travel provided to military personnel from Ft. Leonard Wood, Missouri, to Lambert International Airport in St. Louis, Missouri. The MOA was in effect from September 4, 2018, and was not to exceed January 11, 2019. Payment arrangements between Ft. Leonard Wood MWR and Vandalia for past services were facilitated via paper check. Ft. Leonard Wood is located within the Western District of Missouri.

13. On January 16, 2019, an e-mail that appeared to be from "dennisstreif@vblinc.com" was sent to Chloe Williams ("Williams"), MWR Leisure Travel Office Business Manager. Dennis Streif ("Streif") was a Vice President of Vandalia. The e-mail asked if Vandalia could change the payment method from check to an electronic fund transfer ("EFT"). MWR agreed to the payment change and sent a form to the e-mail address dennisstreif@vblinc.com. This form was completed and e-mailed back to Williams from the dennisstreif@vblinc.com e-mail address providing bank account details for a savings account with J.P. Morgan Chase ("JPMC"), number ending XXXXX41030. Upon later forensic review of this e-mail communication, the investigation revealed that the reply from MWR was routed to a spoofed e-mail account, dennisstreif.vblinc@outlook.com.

14. A "spoofed" e-mail is an e-mail address structured to look like a legitimate e-mail address for the purpose of defrauding individuals who may work for an organization or conduct business with an organization. This type of fraud scheme is known as a Business Email Compromise.

15. Following this e-mail exchange, on January 25, 2019, MWR caused three EFTs to be distributed from MWR's Wells Fargo Bank account to the aforementioned JPMC savings account, XXXXX41030. On January 28, 2019, the three EFTs were deposited into the JPMC savings account XXXXX41030. The three transfers, totaling $164,568 in non-appropriated MWR funds, are detailed below:

a. Automated Clearing House ("ACH") Trace #8170366

i. Amount: $76,544.00

ii. Originating financial institution: Wells Fargo

iii. Receiving financial institution: JPMC

b. ACH Trace #8170370

i. Amount: $4,000.00

ii. Originating financial institution: Wells Fargo

iii. Receiving financial institution: JPMC

c. ACH Trace #8170368

i. Amount: $84,024.00

ii. Originating financial institution: Wells Fargo

iii. Receiving financial institution: JPMC

16. On February 21, 2019, Melissa Kaemmerer ("Kaemmerer") of Vandalia Bookkeeping contacted Williams because Vandalia had not received any payment related to the current MOA. Williams shared the January 16, 2019, and subsequent e-mails from "dennisstreif@vblinc.com." Kaemmerer stated she was only privy to the e-mails regarding Ft. Leonard Wood MWR Exodus that were forwarded to her by Streif. Kaemmerer identified that several details in the e-mails, such as Streif's telephone number, were incorrect and she confirmed the e-mails provided the wrong banking institution and bank account information. Kaemmerer advised that Vandalia uses UMB Bank, not JPMC. After reviewing the e-mails, some of which actually included a reference to dennisstreif.vblinc@outlook.com, Kaemmerer identified such e-mail address and advised that this was not a valid Vandalia e-mail address.

17. Based on Williams' conversation with Kaemmerer on February 21, 2019, Williams told Kaemmerer she would have the payments recalled.

18. On February 24, 2020, Vandalia leadership gave consent to DCIS to search any electronic device that could have been involved in the transaction between Vandalia and MWR. DCIS received written consent from Vandalia to image four desktop computers. DCIS collected

four forensic images, including one of Streif's computer, and submitted the images for analysis by the Defense Cyber Crimes Center.

19. During an interview with Streif, he stated that in October of 2018 he received an e-mail at his Vandalia e-mail account dennisstreif@vblinc.com to log in and verify his Microsoft Outlook credentials. A forensic examiner with the Defense Cyber Crimes Center conducted the analysis of the forensic image of Streif's computer. The e-mail presented itself as an Outlook password reset e-mail. Streif opened the e-mail and followed a hyperlink, which resulted in the theft of Streif's login credentials to his Vandalia e-mail account. A forensic analysis determined that on October 25, 2018, Streif accessed a website hasuik.com, where Streif entered his Outlook e-mail credentials. Hasuik.com's Internet Protocol ("IP") address is listed as 186.64.114.60, which I later found to be registered in Chile. This allowed an unknown subject ("UNSUB") to gain access to Streif's e-mail account.

20. From January 16, 2019, thru January 17, 2019, the UNSUB began an e-mail exchange with MWR from dennisstreif@vblinc.com. The UNSUB inserted a rule which re-directed all replies from Streif's e-mail account dennisstreif@vblinc.com, to dennisstreif.vblinc@outlook.com.

21. A "rule" is a cyber-security term used to describe execution instructions for a program or task. In this case, the UNSUB changed the rules (e-mail settings) that a recipients' reply would be redirected to the spoofed e-mail address dennisstreif.vblinc@outlook.com instead of dennisstreif@vblinc.com.

22. Forensic analysis of an e-mail from dennisstreif.vblinc@outlook.com via IP 216.69.139.30 to MWR was identified to contain an attachment "New 2016 US BANKING ONLY EFT form.xlsx." This attachment contained routing and account numbers information for two

JPMC accounts. The mail header identified the "to" and "from" information, as well as GoDaddy.com servers involved.

Subject	RE: [Non-DoD Source] Invoice for Charter #55656
Date (Sent)	01/17/19 12:12:51
mail Headers	X-Priority: 3 (Normal) Content-Type: multipart/mixed; boundary="---------- 050407050405010706050700" To: Williams, "Chloe E NAF USARMY USAG (US)" <chloe.e.williams.naf@mail.mil> Return-Path: dennisstreif@vblinc.com From: "dennisstreif@vblinc.com" <dennisstreif@vblinc.com> Subject: RE: [Non-DoD Source] Invoice for Charter #55656 Received: from UHIL3CPA05.eemsg.mail.mil (152.229.121.197) by edge-okcd01.mail.mil (152.229.52.103) with Microsoft SMTP Server id 14.3.408.0; Thu, 17 Jan 2019 12:14:41 +0000 Received: from utinhpaoc.easf.csd.disa.mil (152.229.52.103) by UTINHPANU.easf.csd.disa.mil (152.229.52.41) with Microsoft SMTP Server (TLS) id 14.3.408.0; Thu, 17 Jan 2019 12:14:42 +0000 Received: from p3plsmtp26-04-2.prod.phx3.secureserver.net (HELO p3plwbeout26-04.prod.phx3.secureserver.net) ([216.69.139.30]) by UHIL3CPA08.eemsg.mail.mil with ESMTP/TLS/DHE-RSA-AES256-SHA256; 17 Jan 2019 12:13:23 +0000 Received: (qmail 136881 invoked by uid 99); 17 Jan 2019 12:12:51 -0000 Received: from p3plgemwbe26-03.prod.phx3.secureserver.net ([10.36.144.22]) by :WBEOUT: with SMTP id k6XTgxcZ4nPAFk6XTgeGGf; Thu, 17 Jan 2019 05:12:51 -0700 Reply-To: "Dennis Streif <dennisstreif@vblinc.com>" <dennisstreif.vblinc@outlook.com> Date: Thu, 17 Jan 2019 06:12:49 -0600 Message-ID: <20190117051249.7c2a766df86dc87dc3236e0d81d54730.39f9c19dfd.wbe@email26.godaddy.com> MIME-Version: 1.0 X-Mailer: Microsoft Outlook 15.0 Thread-Index: AQHUrl32hy5txUc7RxOqXDoWy6vUpQ== Content-Language: en-us x-ms-exchange-organization-authas: Anonymous x-ms-exchange-organization-authsource: utinhpaoc.easf.csd.disa.mil
Impersonation Content	"Chloe, Please find attached **ACH** form again, there was an error trying fill it out yesterday as we entered our Old checking account. Hope it has not been submitted to the accounting team? We are sorry for the inconvenience this may have caused. Please find our correct ACH savings account in the form attached and get back with remittance details.
	Please get back to me if you have any question. Dennis Streif (618) 344-2172 ext 243 direct"

File Name	MD5 Hash	Content
New 2016 US BANKING ONLY EFT form.xlsx	9048095bf6b4fb383e1bde840180bac5	JP Morgan Chase Bank Chase Bank, 270 Park Avenue, New York, NY 10017, USA Routing: 267084131 Account: 3808641030 (Savings) Contact Person: Dennis Streif Phone: (618) 344-2172

23. Microsoft records associated with the dennisstreif.vblinc@outlook.com e-mail account were reviewed. These records indicate the account was created on December 17, 2018. The account owner was identified as "Dennis Streif." The account was accessed from various IP addresses between December 18, 2018, and July 18, 2019. The IP addresses originated in Nigeria.

24. As a part of the investigation, bank records associated with JPMC savings account XXXXX41030 were reviewed. These records showed that Franklin Huggins ("Huggins") opened the account on December 11, 2018. Subsequent records received from JPMC related to Huggins showed that he also opened bank account XXXXX16232 with JPMC on the same date.

25. Additionally, a review of the records associated with Huggins' JPMC checking account XXXX16232 revealed several transactions between January 3, 2019, and January 9, 2019. These transactions included a large deposit made to the account on January 3, 2019, for $49,859.00, and the subsequent purchase and issuance of two cashier's checks on January 4, 2019, in the aggregate amount of $45,300.00. Huggins was identified as the purchaser of the cashier checks via a signed JMPC withdrawal slip dated January 4, 2019.

26. MoneyGram transactions between January 4, 2019, and January 5, 2019, also correspond with information derived from JPMC records regarding Huggins. For instance, JPMC records from checking account XXXX16232 reflected transactions on January 4, 2019, at a Walmart Supercenter located in Ocala, Florida for $3,503.52; on January 5, 2019, at a Walmart Supercenter located in Homosassa, Florida for $250.88 inclusive of $100.00 cash back; and on January 5, 2019, at the same store for $235.71. Transaction information provided by Walmart reflected debit card transactions for four money orders in the value of $3,500.00, plus fees, on January 4, 2019. The Walmart data further showed another money order purchase conducted on

January 5, 2019, in the value of $150.00, plus fees. The remaining transactions identified at Walmart for the $235.71 appeared to be for items of a personal nature.

27. JPMC account internet access logs showed a profile username of "letmemakecash2" associated with the e-mail address frankhugginse5@yahoo.com ("Subject Account") accessing the aforementioned accounts. The JPMC accounts were accessed electronically multiple times between December 11, 2018, and January 23, 2019, under this profile. Records from JPMC indicated an IP address of 97.76.106.58 connected to Huggins' JPMC account over the course of several days beginning December 14, 2018. The log-in records show the times of access typically between the hours of 2200 and 0800 Eastern Time. Records from Charter Communications showed the IP address belonged to Seven Rivers Regional Medical Center, of Crystal Rivers, Florida. Based on employment records from the state of Florida, Huggins has been employed by a medical staffing company since 2017. Other records received by investigators showed that Huggins used an address in Homosassa, Florida as his residence during December 2018 through January 2019. Ocala, Florida, Homosassa, Florida, and Crystal Rivers, Florida are all located in close geographical proximity to each other.

28. Given the e-mail suffix, I know that Yahoo is the entity serving as the e-mail provider. Through my research, I found that Yahoo is a subsidiary of Oath Inc. d/b/a Verizon Media, located at 701 First Avenue, Sunnyvale, California 94089.

29. JPMC records further identified that Huggins made a phone call to JPMC on January 24, 2019, regarding the savings account ending XXXXX41030. The records indicated that a separate phone call from an unidentified person was made to JPMC on January 29, 2019, inquiring about access to funds in the account ending XXXXX41030.

30. A 2703(D) preservation letter and subpoena for subscriber information in regards to the Subject Account was previously served via Law Enforcement Online Submissions on March 2, 2020. Login information provided by Oath Inc. d/b/a Verizon Media showed 81 logins identified for the Subject Account from March 8, 2019, through February 25, 2020. A login was identified for the Subject Account via IP 97.76.106.58 on May 15, 2019 at 07:50:59 UTC.

31. On April 30, 2020, Lisa Hoke, Senior Banking Officer, Installation Management Command, United States Army Banking, Investment and Insurance, Joint Base San Antonio, Texas, confirmed MWR received three EFTs totaling $164,568.00. The funds were returned from JPMC in response to an Originating Financial Institution request.

THE SUBJECT ACCOUNT

32. Based on my training and experience, and a review of evidence to date, I believe probable cause exists that Franklin Huggins controlled the JPMC bank account that received the $164,568 from MWR after an unknown subject gained access to Dennis Streif's Vandalia e-mail account and caused such funds to be transferred to the JPMC account. A user profile was created to electronically access the JPMC savings account that held this money, which used frankhugginse5@yahoo.com to set up such account. Therefore, probable cause exists that such e-mail address was used to facilitate access to the JPMC account that received the MWR funds and, thus, was used to facilitate this fraudulent scheme.

33. Through the above information uncovered during my investigation, I believe that probable cause exists that Huggins has committed the crimes of false claims (18 U.S.C. § 287), conspiracy (18 U.S.C. § 371), wire fraud (18 U.S.C. § 1343), 18 U.S.C. § 1956 (money laundering), and 18 U.S.C. § 1957 (money laundering), and that he utilized the e-mail address of frankhugginse5@yahoo.com ("Subject Account") to do so. Specifically, there is probable cause

that Huggins opened a checking and savings account at JPMC on December 11, 2018, and conspired with unidentified individuals to spoof the e-mail address of a Department of Defense contractor, Vandalia, to e-mail the Ft. Leonard Wood MWR, and through that e-mail, requested a change of EFT information to route $164,568.00 in MWR payments to the newly opened JPMC account in Huggins' name.

BACKGROUND CONCERNING E-MAIL

34. For the account referenced in this affidavit, I have served the relevant provider with a preservation letter pursuant to 18 U.S.C. § 2703(f). In general, an e-mail that is sent to an e-mail provider's subscriber is stored in the subscriber's "mail box" on the e-mail provider's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on the e-mail provider's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on the e-mail provider's servers for a certain period of time.

35. Yahoo is an online internet based service provider, which offers its users e-mail account(s) services, instant messaging, messaging alerts, and other messaging/communication based services. All of these services utilize the internet as a means of conveying and receiving data, including but not limited to e-mail, instant messages, and message alerts.

36. In my training and experience, I have learned that social media companies, like Yahoo, provide a variety of online services, including electronic mail ("e-mail") access, to the public. These e-mail service providers allow subscribers to obtain e-mail accounts at the company's own domain names (such as gmail.com, yahoo.com, or icloud.com), like the e-mail accounts listed in Attachment A. Subscribers obtain an account by registering with these e-mail providers. During the registration process, these e-mail service providers ask subscribers to provide basic personal information. Therefore, the computers of these companies are likely to

contain stored electronic communications (including retrieved and un-retrieved e-mail for the e-mail subscribers) and information concerning subscribers and their use of these e-mail provider's services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. In addition to e-mails, a subscriber to Yahoo can also store with the provider other electronic media, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by the e-mail service provider. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

38. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

40. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an e-mail account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy"

while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described below, e-mail providers typically log the IP addresses from which users access the e-mail account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the e-mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Last, stored electronic data may provide relevant insight into the e-mail account owner's state of mind as it relates to the offense under investigation. For example, information in the e-mail account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION AND REQUEST FOR SEALING

42. Based on the forgoing, I request that the Court issue the proposed search warrant.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Oath Inc. d/b/a Verizon Media (Yahoo). Because the warrant will be served on Oath Inc. d/b/a Verizon Media (Yahoo), who will then compile the requested records at a time

convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Nick Masellis
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to before me in my presence via telephone on this 22nd day of September 2020.

Honorable David P. Rush
Chief United States Magistrate Judge